ワークショップ
開催案内

Workshop on Recent Developments of Multivariate Public Key Cryptosystems

●開催趣旨

総務省の 2008 年度研究プロジェクト SCOPE の 1 つとして、「量子コンピュータの出現に対抗し得る公開鍵暗号の研究」(研究代表者 辻井重男)が採択され、鋭意研究を推進しております。

この度、その一環として多変数公開鍵暗号（MPKC）について、活発な研究活動を推進している、米国シンシナティ大学の J．Ding 教授をお招きして、東京および大阪において、下記のワークショップを開催することといたしました。

MPKC は日本生まれの公開鍵暗号です。ご参加をお待ちしております。

Jintai Ding, Ph.D
Professor of Mathematics, Department of Mathematical Sciences,
University of Cincinnati

◆東京開催

開催日時：平成 21 年 2 月 19 日（木）　10：00 ～ 18：00
会場：中央大学後楽園キャンパス　3号館　3階　３３０９号室

◆大阪開催

開催日時：平成 21 年 2 月 23 日（月）　10：00 ～ 17：00
会場：大阪学院大学　2 号館　4 階　会議室（02-04-02）

●参加申込方法

1)参加申込は、準備の都合上事前にお申込ください。
2)ご氏名･勤務先名または大学名をご記入の上お申込ください。
参加申込先 ： CRYPT2009@tamajs.chuo-u.ac.jp

➢　プログラムは裏面です。

● プログラム

SCOPE　WORKSHOP on POST QUANTUM CRYPTOGRAPHY in TOKYO

Program

10:00—11:30　Prof. J.Ding　Mutant XL algorithms.

11:40—12:20　S. Tsujii　2-layer Nonlinear Piece In Hand Method for Various MPKC

12:20—13:30　Lunch

13:30—14:10　Mr. Daniel Cabarcas　Mutant F4 algorithm

14:10—14:50　K. Tadaki　An Exact Analysis of Rank Attacks

14:50—15:30　M. Gotaishi　Proposal of HXL Algorithm

15:30—15:50　Coffee Break

15:50—16:30　K. Akiyama　On the algebraic surface cryptosystem

16:30—17:10　T. Matsumoto　How I Conceived the Cryptology with Systems of Multivariate Polynomials as Public Keys

17:10—17:50　K. Kurosawa　Truly Efficient 2-Round Perfectly Secure Message Transmission Scheme

SCOPE　WORKSHOP on POST QUANTUM CRYPTOGRAPHY in OSAKA

Program

10:00—10:10　Opening　Address　S.Tsujii　&　M.Kasahara

10:10—11:20　M. Kasahara　Application of Error Correcting Codes for Constructing Multivariate PKC

11:20—12:00　S.Tsujii　Development of Piece In Hand Method for MPKC

12:00—13:00　Lunch

13:00—14:00　Prof. J. Ding　Multivariate Public Key Cryptosystems over Odd Characteirstics

14:00—14:40　A. Hayashi　On the multi point communication over a knapsack cryptosystem

14:40—15:20　K. Kobayashi　A Knapsack Cryptosystem Resisting Well-known Attacks

15:20—15:50　Coffee Break

15:50—17:00　Discussion with Prof. Ding and Mr. Daniel Cabarcas